

## Indiana University professor examines how school violence was averted

*The most prominent finding involves building relationships -- so every student had an adult to whom he or she could turn, and a close relationship between schools and local police*



Staff at schools that experienced “near misses,” where violence was averted in student-to-student hostage situations, often attribute their success to luck. But a little prodding by an Indiana University Bloomington education professor has revealed that the teachers and staff already had taken steps that worked in their favor at those crucial times.

Research on school violence typically examines situations where shootings or other forms of violence occurred. Jeff Daniels, an assistant professor in the Department of Counseling and Educational Psychology in IUB’s School of Education, is pursuing a different angle -- learning as much as he can about how nightmarish situations ended without a shot.

Daniels said the most prominent finding involves building relation-

ships. The four schools he examined had policies in place that required teachers and staff to go out of their way to get to know students and to make sure every student had an adult to whom he or she could turn.

“These students (perpetrators) were not unknown,” Daniels said, explaining that in many incidents of actual school violence, school authorities were not familiar with the perpetrators.

In the schools Daniels examined, teachers and staff established relationships with students in a variety of ways, including eating lunch with them, talking to them in the hallways and attending extracurricular activities. Other key findings include the following:

- Training is crucial. In all four incidents, teachers, security officers and administrators involved in the incidents had prior crisis training that involved lock downs and other drills.
- The schools had close relationships with local police. Three of the schools had an officer on campus at all times. The fourth employed a resource officer with a background in law enforcement.
- School authorities must be aware of what’s going on in the schools. An important source of information, Daniels said, is the students. In one incident, a student who was late for class recognized a stu-

dent on campus who had been expelled and should not have been on campus. The student told the principal, who initiated a lock down. The expelled student ultimately held a classroom of students hostage using knives.

A student used a gun to hold a classroom of students hostage in another incident. The principal, who knew the perpetrator, talked the student into surrendering. The resource officer, who also was in the room, never had to draw his gun.

Daniels interviewed teachers, administrators and security officers involved in incidents at three high schools and one middle school in the last two years. Three of the schools, which are not named in the research, are smaller, rural schools. The fourth is a larger, urban school. In the hostage situations, one student took a class hostage using a gun; in a particularly volatile situation, the expelled student took a class hostage using two kitchen knives, lunging at a principal and threatening a student; and a middle school student took another student hostage, using a knife and a gun, and attempted to leave the building. In the fourth situation, school authorities foiled a Columbine-like attack.

Daniels plans to interview staff at two more schools. Another phase of his research involves talking with perpetrators to find out “why they

(Continued on Page 3)

# An Interview with Lt. Col. Dave Grossman

*A review of the new book, "On Combat: The Psychology and Physiology of Deadly Conflict in War and in Peace," by Lt. Col. Dave Grossman with Loren W. Christensen*

With the release of the long awaited book, "On Combat," TUEBOR has taken the opportunity to interview author Lt. Col. Dave Grossman, a retired U.S. Army Ranger and Pulitzer nominated writer of "On Killing" and "Stop Teaching Our Kids To Kill." Dave has become a national figure in the cause against violence and the education of police officers. Going back to his days as a professor at West Point Military Academy, Dave teaches a concept he calls the "Bulletproof Mind."

*Tuebor: Can you tell us the objective of your new book "On Combat," and the concept you call the Bulletproof Mind?*

Dave: The LEO has spent countless days on the range and in training, and years of practical experience on the streets, learning to survive the felonious assault. But we are far more likely to be destroyed by the stress after the incident. In WWI, WWII, and Korea, we lost more boys to psychiatric casualties than were killed by the enemy. In the LE community we lost about 60 cops to felonious assaults last year, but we lost hundreds to suicide, and that is just the tip of the iceberg of those destroyed by the stress of this job. Thus the goal is to send out a generation of mentally prepared and informed warriors.

*Tuebor: The police officer's authority revolves around the Bill of Rights, with "burden of proof" and "minimum use of force" standards. Does this fit with military research?*

Dave: When it comes to the psychology and physiology of combat, there is a universal body of knowledge that applies to all aspects of the warrior community. A recent article in the FBI Law Enforcement Bulletin reinforced the point that "the type of trauma experienced by soldiers in combat is quite similar to that endured by law enforcement officers." The point is that anything you can do to enhance police, mentally and physically, also improves performance.

*Tuebor: What do police need to know regarding their own physiological and psychological responses to danger?*

Dave: The most important thing to know is the incredible, overwhelming response of the body in extreme fear/survival stress situations. Once you KNOW about these things, you are far better prepared to deal with them – forewarned is forearmed. The next step is to learn how to PREVENT these extreme physiological responses. The final step is to understand what to expect AFTER the stressful situation, how this can lead to PTSD and how to prevent stress disorders.

*Tuebor: You discuss "Perceptual Distortions" in your book. Is this something that police can minimize?*

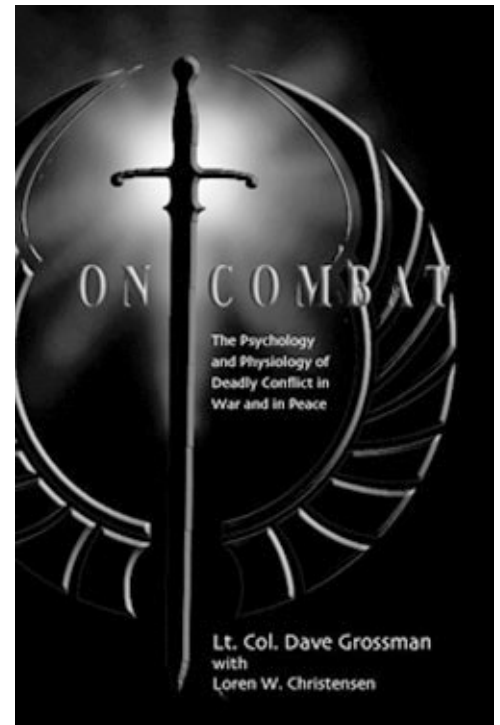
Dave: Yes. By reducing stress responses we can reduce this. Stress inoculation, mental mindset, autopilot/conditioned response, tactical breathing, these are just some of the vital skills needed by police.

*Tuebor: What advice can you give for law enforcement training?*

Dave: The most important thing is realistic training. Simunitions-type force-on-force training is to the LEO what the flame house is to the fire fighter, or the rappel tower is to the mountain rescue climber. We must be inoculated against the stressors we will face, and the more realistic the training (and the stress thereof) the greater the inoculation, and the greater the self-control in the real event. Likewise, we must realistically train officers to "communicate" in stressful situations, so they can talk people out of violence when it's safe and possible to do so.

*Tuebor: While there is important new emphasis on anti-terrorism, we don't want to neglect all the other public safety issues. Has anything changed regarding school violence and the effort to raise well-adjusted kids?*

Dave: Last year we had an all time record number of dead from violent attacks in U.S. schools. And I fear that whatever is happening in the schools, we will reap in the workplace and community in the years to come. The most important thing on that front is



the Stanford University Medical Department research demonstrating that if we convince the kids to turn off the TV and video games, then (as was demonstrated in a controlled experiment) we will see a 40% reduction in violence and a 50% reduction in bullying in one semester! More information about this Stanford "SMART Curriculum" can be found at [www.sosparents.org](http://www.sosparents.org). This is something that gives us real hope for the future. By the way, Escanaba, Michigan, is one of the first school districts in the U.S. to put this curriculum in place in all of its schools, and they demonstrated a 55% reduction in violence!

*Tuebor: What is your concept of the Peace Warrior?*

Dave: I had the privilege of being the co-keynote speaker with a Nobel Peace Prize recipient at an international peace conference. There I proposed the term peace warrior to refer to those in every profession, with and without guns, who are dedicated to moving our world forward toward peace. This term has been in use for a long time, and today it is widely accepted. It includes the Red Cross, the non-governmental organizations in a war zone, the probation and parole

(Continued on Page 3)

(Continued from Page 2)



officers, the doctors and EMTs, the firefighters, the social workers, and even the clergy. So where do we get such men and women? We build them. We train them. We nurture them. There can be no more important or noble endeavor for a civilization.

*Tuebor: Lastly, what advice can you give police related to homeland security?*

**Dave:** It's obviously important to look for signs, to prevent what we can, but to also be prepared, to have a plan. If they came to your kid's school tomorrow, would you be ready? Denial is our greatest enemy. Denial makes us physically and psychologically unready at the moment of truth.

*Tuebor: Thank you for taking time to conduct this interview.*

**Dave:** My sincere pleasure – "The bravest are surely those who have the clearest vision of what is before them, glory and danger alike, and yet notwithstanding, go out to meet it!" – Thucydides

## Lowering Stress Induced Adrenaline Overloads

### The Key to Increasing Officer Safety & Reducing Over-Reactions

An officer's worst enemy is adrenaline overload. A felony warrant comes back – the "stress" during an apprehension, the "excitement" of a chase – any number of events can cause an officer's adrenaline level to soar.

Once the huge adrenaline dump occurs, things can go bad to worse. Tunnel vision and/or target fixation can set in. Fine and complex motor skills diminish, and the reasoning part of the brain can be severely hindered.

A lot of police training classes now teach breathing exercises for stress control. The breathing technique, known as Chi or Sanshin breathing in martial arts, or autogenic breathing, has been touted as "combat breathing" in police training circles.

The breathing is done in cycles.

- Breath in through your nose for a count of four;
- Hold your breath for a count of four;
- Exhale through your mouth for a count of four;
- Hold your breath for a count of four, and then restart the cycle.

This simple technique will lower your blood pressure, stress level, and minimize the overwhelming side effects of adrenaline.



### THE MISSING PIECE OF THE PUZZLE

The big missing piece of the puzzle is: How do we teach it so officers remember to do it when they need it most? Well, you probably can't, teach them to "remember" to do it, that is. You can, however, make it a conditioned response to a specific stimulus. Or as Bruce Lee once quoted a teaching, "Learn it until you forget it."

The methodology of this training is quite simple. Every time you hear a siren, the officer practices combat breathing. Every time! Or for that matter, every time the officer removes his weapon on the range, the officer practices combat breathing. Every time you could "potentially" become involved in a high stress situation, practice it. This way, when the real deal comes along, you instinctively combat breath.

The analogy that is often used with this is riding a bicycle. Difficult to learn, have to practice and practice, will fall (fail) several times, but once you learn it, you never forget how.

Your mind is the primary source of every positive, and negative, action you make. Your brain is the little voice in your head that makes your body accomplish tremendous acts of bravery under unthinkable situations. Combat breathing is just one useful tool that will bring out your best. The rest is up to you!

Article by Sgt. Charles E. Humes, Jr. <http://hometown.aol.com/nodonuts>, published in "Integrity Talk," the official publication of the International Association of Ethics Trainers [www.ethicstrainers.com](http://www.ethicstrainers.com).

(Continued from Page 1)

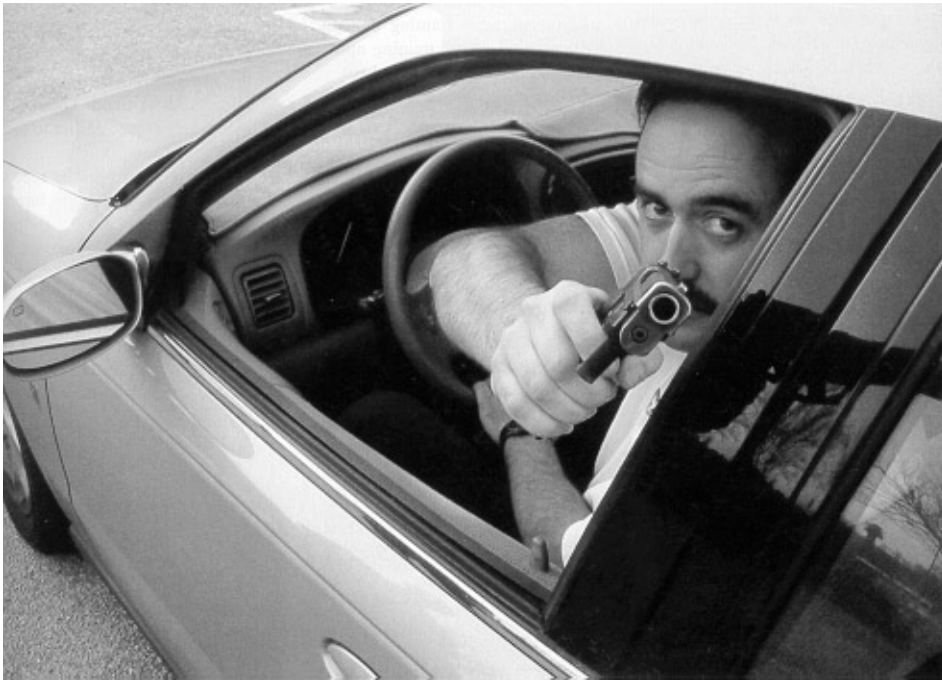
didn't shoot." As part of this, he will talk with students at schools that experience near misses to get their perspectives. He wants to accumulate enough information to create a violence prevention program that covers such issues as warning signs and hostage negotiation training.

Daniels presented his findings recently at the annual meeting of the American Psychological Association. He will report findings this fall at a convention of the American Society of Criminology.

Article released Sept. 22, 2004. For more information, contact Jeff Daniels, School of Education, at 812-856-8304 or [jedaniel@indiana.edu](mailto:jedaniel@indiana.edu). Web version of this report can be found at: Indiana University <http://newsinfo.iu.edu/news/page/normal/1657.html>.

Michigan State Police Prevention Services Section, 517-333-4006.





## Traffic Stops: Be Professional, Be Safe!

Every stop for a traffic violation has the potential for danger. Routine traffic stops, as they are often called, sometimes turn out to be anything but routine. But treating every traffic stop as a high-risk felony also has its problems. At many agencies, more complaints generate from traffic stops than from any other form of citizen contact. Officers need to be courteous and professional – but also safe! The secret is to treat all motorists with dignity, but plan for danger. Here are some tips:

**1. EXIT QUICKLY – APPROACH CAUTIOUSLY.** Statistics show that officers are most vulnerable sitting in the car, and when they walk up on the stopped vehicle. But a potential attacker will often be deterred if an officer looks like he or she is prepared for action. Exit quickly, but approach cautiously.

**2. READ THE SCENE.** Continually watch for furtive or suspicious movements in the target vehicle. Consider alternative approaches. Plan an avenue for retreat or cover if danger presents itself. Protect your weapon and be prepared to use it, if necessary.

**3. ACT PROFESSIONAL – LOOK FOR DANGER.** Always present yourself in a confident and polite manner – in speech and bearing – while constantly looking for signs of danger. Two-way

communication is an opportunity to detect contradictions and indicators of criminal activity. Two-way communication is also a means to build better community relations with law respecting citizens.

**4. STAY DISCIPLINED IN THE FACE OF PROVOCATION.** Don't let subjects distract you by allowing them to instigate an argument. Treat belligerence with suspicion and remain disciplined. If suspicion builds where you decide to ask for a consent search, communicate in word and tone of voice that indicates this is a request – not a command. Also remember that the driver may withdraw the consent for a search at any time. Don't hesitate to call for back-up, and try to wait for your back-up during a search or arrest situation.

**5. REPEAT STEPS 1-4 ON SECONDARY CONTACTS.** When returning to the stopped vehicle for a follow-up contact, repeat steps 1-4. Just because things have gone well so far doesn't mean you should drop your guard. Many attacks on officers occur on the second approach because the culprit thinks the officer discovered something during the radio check.

For every traffic stop, police officers need to be prepared for friend and foe alike. Acting professional while looking for danger is one tactic that is a constant.

*“We police play by the rules... even though the bad guys have no rules.” – Deputy Ray Essary*

“This is the destiny of democracy, as not all means are acceptable to it, and not all practices employed by its enemies are open before it.

Although a democracy must often fight with one hand tied behind its back, it nonetheless has the upper hand. Preserving the Rule of Law and recognition of an individual's liberty constitutes an important component in its understanding of security. At the end of the day, they strengthen its spirit and allow it to overcome its difficulties.”

- Israeli Supreme Court, in a 1999 ruling to prohibit torture or physical pressure during interrogations.



## *Cops are the key:* The “Broken Windows” Tactics That Sliced Crime Can Work Against Terrorism

If you want to fight the war on terror and win, then you want to talk to George Kelling. He’s the Rutgers University professor who authored the seminal “broken windows” theory of law enforcement, with UCLA crime guru James Q. Wilson. It prompted a sea change in local policing in the 1990s, helping make millions of Americans safer.

### **BROKEN WINDOWS AGAINST CRIME**

Cracking down on terrorism, Kelling argues, is akin to when the police started going after quality-of-life offenses a decade ago. That was when the Police Department put “broken windows” – the idea that criminals are less able and eager to commit major crimes when minor crimes are no longer tolerated – into full-blown execution.

“Not everyone who urinates in public is a criminal, but we found there are an awful lot of criminals who urinate in public,” explains Kelling. That approach worked wonders in city subways. From 1990 to 1992, subway crime plummeted an astonishing 30% as arrests and expulsions soared from 2,000 a month to between 10,000 and 15,000 a month. Much of that involved enforcement of laws against what were then considered minor infractions, like turnstile jumping.

It turned out that one in six jumpers was carrying a weapon or was wanted for another crime. All too often, fare-beaters were the same people who were sticking up passengers, picking pockets and snatching gold chains.

### **BROKEN WINDOWS AGAINST TERRORISM**

Like any criminal, “Terrorists have to commit many minor crimes in order to be able to commit major acts of terror,” says Kelling. “Those crimes include crossing borders illegally, money laundering, ID theft, credit card theft, and plenty of document forgeries. All of that makes them vulnerable to intervention by law enforcement.”

Terrorism’s equivalent are the border-hoppers – those who illegally cross into the U.S. with fake passports or through the many gaping holes along our borders. Following the Kelling dictum, not everyone with forged documents is a terrorist, but a heck of a lot of terrorists are carrying forged documents.

### **DISCRETION IS CALLED FOR**

Kelling maintains that officers must and should exercise discretion in all situations, including the search for terrorists. Giving police officers permission to use their professional judgment is not the same as endorsing random or arbitrary policing.

Police work is in transition, says Kelling. Their role in the justice process requires even “greater” commitment to developing policy guidelines that set standards and shape the inevitable use of discretion that reflect community values.

### **CONCLUSION**

If you want to unearth the terror cells in our homeland, says Kelling, you’d do better with police agencies. Whether a terrorist is from a foreign country or is a local nut, Kelling says that once a terrorist is inside the country, the best tool for finding and apprehending them is the police. “Go local,” he urges.

The real intel is in the cities, in the neighborhoods. The culprits conducting video surveillance of the stock exchange have to live somewhere. The police are more frequently involved in creating and nurturing partnerships with community residents, businesses, faith-based organizations, schools, and neighborhood associations. Police have their ears to the ground. They can find the bad guys. Police can enforce the low-level crimes that will ultimately net the big fish.

*Sources: New York Daily News, 8/4/04, and The National Institute of Justice, “Broken Windows and Police Discretion.”*



# FRAUD ON THE INTERNET:

*Signs your PC's under siege, and what you can do!*

## IS YOUR HOME PC A ZOMBIE?

Are hackers using your PC to spew spam and steal? Since early 2003, wave after wave of infectious programs have begun to saturate the Internet, causing the number of PCs hijacked by hackers and turned into so-called "zombies" to soar into the millions. And, much like zombies of voodoo legend, they mindlessly do the bidding of their masters and help commit crimes online.

Using zombies to broadcast spam for Viagra or quickie loans has emerged as a huge business. Yet spreading ordinary spam is actually one of a compromised computer's more benign tasks.

Bigger spoils lie in using zombies in elaborate "phishing scams," in which e-mail directs consumers to bogus Web pages to trick them into surrendering personal information.

## PHISHING SCAMS

First seen more than a year ago, phishing scams begin with e-mail messages broadcast to potential victims. The e-mail directs them, often under the guise of doing a security check, to a bogus Web page with the identical look and feel of an authentic page.

A network of zombie PCs (maybe your PC), e-mails the original request to tens of thousands of potential dupes. A separate zombie, usually a more powerful PC, often sitting in a remote country, perhaps in an obscure nook at a university, serves up the counterfeit Web page. Another zombie, in yet another country, perhaps in the basement of a small shop, stores the stolen account details and conducts the theft.

## TROJAN HORSES

Web "contagions" are waiting to infect your home PC on numerous high-traffic Web pages across the Internet. Most do the basics: plant a back-door Trojan horse and turn over full control to an intruder who might be sitting half a globe away.

Some have begun implanting spyware called "keystroke loggers," which are designed to notice whenever the PC user types anything that looks like account information. It grabs the information and sends it to a zombie

computer for storage and risk-free access by the crooks.

The scariest type of attack is one most consumers aren't aware of. Scores of sophisticated programs, called "worms" and "bots," continually scour the Internet for Windows PCs with security holes. There are hundreds of Windows vulnerabilities, and new ones turn up regularly. Microsoft issues software patches, or fixes, each month for the most troublesome. But most home users, and many businesses, don't keep up to date on patches.

## SYNDICATE CYBERCROOKS

Sneaky cybercrooks are finding it profitable to "be patient and nick an account for a long time," says Dan Larkin, unit chief of the FBI's Internet Crime Complaint Center.

Computer networks make this easy to do since they form a virtual world in which footprints and fingerprints are easily erased at a distance. Experts say clues point to loosely organized crime syndicates, probably in Russia, Latvia, Kazakhstan and China, coordinating phishing scams with other schemes. Another threat, terrorists stealing account information to finance their crimes.

In what feds call one of the biggest phishing busts, a Romanian man was arrested last year and convicted for using an elaborate network of bogus Web pages and escrow accounts to fleece Americans out of \$500,000.

## FILCHING FINANCIAL INFO

Typically, filched financial information, such as credit card numbers, is sold on Web sites. Buyers often use card numbers to make long-distance phone calls, sign up for pornographic sites and buy computers over the Internet.

Phishing attacks have surged more than 10 times since January, and U.S. victims have lost an estimated \$2.4 billion from phishing in the 12 months ending in April, according to market research.

## KILLING ZOMBIES AND TROJAN HORSES

If your Windows PC is being used as a zombie, you may notice recurring slowdowns of e-mail and Web browsing. Or you may not be able to e-mail or browse at all. If your PC has been infected with a self-replicating network worm, a dormant backdoor Trojan horse or several other types of stealthy programs, you may not notice anything. To protect yourself, the following PC protection steps are recommended:

- Always use a personal firewall with a PC connected to a cable modem, DSL or wire-

less Internet service. Free ones are listed at [www.free-firewall.org](http://www.free-firewall.org). Tip: Have the personal firewall set to at least the medium level of security.

- Buy anti-virus software, such as Norton AntiVirus, McAfee VirusScan or ZoneLabs Security Suite, and keep the subscription current. Set it to automatically check for updates. Tip: New PCs typically come with a free trial subscription from Norton or McAfee. However, you must subscribe after the trial period expires to continue getting updates.

- Enable Microsoft Windows Auto-Update to automatically download the latest security patches. Tip: Follow instructions to make sure downloaded patches are also automatically installed.

- No software vendor will ever send you patches via e-mail. If you get e-mail pretending to be a patch from Microsoft or any other vendor, delete it. Distrust all attachments. If you have even the slightest doubt, delete it without reading.

- Back up all of your important documents and folders at least once a month, more often if you can stand it. Use complex passwords and periodically change passwords and PINs.

- Beware of spyware. If you can, use the Mozilla Firefox browser. If you must use Internet Explorer (IE), set the security settings to high; this will disable multimedia features of many Web sites, but also will block a main path intruders use to plant Web contagions. Tip: To set IE security to high, navigate to Tools, Internet options, Security settings.

- Install, use and regularly update Lavasoft's Ad-Aware [www.lavasoft.de/english/default.shtml](http://www.lavasoft.de/english/default.shtml) and Spybot Search and Destroy <http://spybot.safer-networking.de/en/index.html> anti-spyware programs. Both are free for the downloading. Tip: Be extremely wary of counterfeit versions of Lavasoft's Ad-Aware, spelled slightly different; those are actually spyware.

Source material provided by Byron Acohido and Jon Swartz, USA TODAY, and the Michigan State Police Computer Crimes Unit.